Week #8- starting from 10th March

Analysis of 3 top layer protocols using the protocol analyser -Wireshark.

What has been done in the previous labs is to understand various concepts of Computer Networks through simulation in a virtual environment. This lab focuses on how to analyse protocols from the live internet.

Step#1 :

Pre-lab activity :

Before entering lab, it is a mandatory for you to read the attached .pdf , [introductionToWiresharkForozan] which is extracted from the text book written by Forouzan.

This write up gives you an introduction to Wireshark and how to use the same.

Step#2:

Lab-activity

1. Invoke Wireshark protocol analyser:

   In Ubuntu based systems in lab, use terminal mode and login as super user.

   Run Wireshark

2. Open the attached trace file [http-ethereal-trace-1]

   To have better understanding in the beginning, we are giving you already captured trace file.

This is a tracefile already captured when a client host has fetched simple html page from a server on the internet.

As you know, while doing this simple task, many protocols at different layers are executed.

Step#3:

You will analyse following 3 protocols in this lab, by reading the captured frames and **answering the questions listed below :**

1) HTTP
2) TCP
3) IP

A. HTTP Protocol analysis

1	How many frames are captured by Wireshark	
2	How may HTTP frames are there ?	
	(To get this information, enter ' http' in the filter field)	

3	Analyse the first **http request frame** (Frame10) and answer the following questions	
3.1	What is the IP address of the HTTP client requesting the page ?	
3.2	What is the IP address of the HTTP Server requesting the page ?	
3.3	Does the client support Google Chrome browser?	
3.4	What is the name of the server from where the page has to be fetched ?	
3.5	Does the client accept .jpeg files ?	
3.6	Is this a persistent connection? If so how long this session can be alive ?	

4	Analyse the **http reply frame** (Frame12) and answer the following questions	
4.1	When was this page fetched?	
4.2	What operating system is run on the server	
4.3	What is the content of the page displayed ?	
4.4	When was the HTML file that you are retrieving last modified at the server?	

B. TCP Analysis

5	**Clear the 'http' and enter 'tcp' in the filter field (Since our focus now is TCP)**	
	Select frame no 7, which is the FIRST TCP segment from the HTTP client to HTTP server. Focus only on TCP PDU	
5.1.	What is the source port address?	
5.2	Prove that this segment belongs to HTTP application layer protocol.	
5.3.	Prove that it is a Connection request segment	
5.4	What is the sequence number of this segment	
5.4	What is the WINDOW size	
	Typically TCP Header is 20 bytes long. In this segment, it shows that header length is 28 bytes. Why ?	

6	**Select Frame 8 which is a TCP reply segment for the Frame 7.**	
6.1	How can you confirm that this segment is a reply for the frame 7?	
6.2	Why is the acknowledge number 1 ?	
6.3.	What is the sequence number ?	
6.4	What are the flag bits set ?	
6.5	Is the window size in the reply is same as that of request from client ?	

TCP uses 3 way handshakes during connection establishment. Find out which frame has the 3rd part of 3 way handshake. [Ans. Frame 9 which has an acknowledgement for Frame8]

C. IP Analysis

7	**Select Frame 7 again, focus only on IP PDU.**	
7.1.	What is the source IP address?	
7.2.	Why is the total length shown as 48 bytes?	
7.3	Can you confirm from that this carries the data given by TCP protocol ?	
7.4	What is the value of ''More' flag bit ? Justify the value ?	
7.5	This datagram goes through a series of routers. Assume that there are no mistakes in the configuration of network and there are no errors anywhere in the network. Still this client may get ICMP message from the network. Do you agree? When can this happen?	